UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,409	12/04/2003	Richard C. Johnson	021756-087310US	7705

51206 7590 12/29/2010

TOWNSEND AND TOWNSEND AND CREW LLP/ORACLE
TWO EMBARCADERO CENTER
8TH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
12/29/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,409	JOHNSON, RICHARD C.	
	Examiner	Art Unit	
	CHARLES C. AGWUMEZIE	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-13,15-19 and 29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-13, 15-19and 29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

12/4/03; 12/17/03; 8/15/05; and 05/09/07

DETAILED ACTION

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 6, 2010 has been entered.

Acknowledgment

2. Applicant's amendment filed on August 6, 2010 is acknowledged. Accordingly claims 9-13, 15-19 and 29-33, remain pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 9-13, and 15-19,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer U.S. Patent No. 5,412,717 in view of Sudia et al (hereinafter "Sudia") U.S. Patent Application Publication No. 2002/0029337 A1 and further in view of

Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 and Tallent JR. et al (hereinafter "Tallent") U.S. Patent Application Publication No. 2006/0179008 A1.

5. As per **claims 9 and 15**, Fischer discloses a computer-implemented method for ensuring non-repudiation of a payment request, the method comprising:

receiving, at one or more computer systems operated by an organization a payment request identifying at least at least one payee;

receiving, at the one or more computer systems operated by an organization, a certificate identifying including certificate-identifying information user-identifying information identifying a user having caused the payment request to be generated, and authority information defining (***see fig. 2, which discloses reference signer's certificate; see col. 6, lines 25-55, which discloses that the signature segment 40 may include a reference to the signer's certificate, i.e., an identifier for identifying the signer's certificate; col. 8,lines 2-25, which discloses that when the program is received by recipient designated by the program, the recipient invokes a copy of the transmitted program to, for example, control the display of the purchase order tailored to the needs of the recipient):***

an authority of the user identified in the user-identifying information to make payment requests (**see fig. 2, which discloses authority invoked for signing; see claim 14, which discloses means for storing at least an indication of the authority granted to the signing party),**

a maximum payment that the user identified in the user-identifying information is authorized to make (**see claim 15, which discloses means for storing data indicating a money**

limit; see claim 16, which discloses wherein said money limit limits the operation of said associated program), and

a list of specific payees to whom the user identified in the user-identifying information is authorized to make payments;

retrieving, with one or more processors associated with the one or more computer systems operated by an organization, stored authority information associated with the user identified in the user-identifying information from a store of authority information hosted outside the organization and that is independent of the received certificate **(col. 6, line 60 – *col. 7, line 10, which discloses that* "Optionally, the authorization signature may also include the digital certificate for the above signatures in a segment 48. Alternatively, such certificates may be accessible from an identified data base (although it may be preferable to include the digital certificates for associated signatures so that signatures may be verified without the need to access any such data base));**

validating, with the one or more processors associated with the one or more computer systems operated by an organization, the authority information within the received certificate based on a comparison between the retrieved authority information and the authority information included within the received certificate **(col. 6, line 60-col. 7, line 10, which discloses that the Alternatively, such certificates may be accessible from an identified data base (although it may be preferable to include the digital certificates for associated signatures so that signatures may be verified without the need to access any such data base))**; and

generating information, with the one or more processors associated with the one or more computer systems operated by an organization, authorizing the payment request in response to a validation of the authority information included within the received certificate when the at least one payee identified in the payment request is included in the list of specific payee defined in the authority information included within the received certificate

6. What Fischer does not explicitly teach is:

receiving, at one or more computer systems operated by an organization a payment request identifying at least one payee;

a list of specific payees to whom the user identified in the user-identifying information is authorized to make payments;

generating information, with the one or more processors associated with the one or more computer systems operated by an organization, authorizing the payment request in response to a validation of the authority information included within the received certificate when the at least one payee identified in the payment request is included in the list of specific payee defined in the authority information included within the received certificate

7. Sudia discloses the method comprising:

receiving, at one or more computer systems operated by an organization a payment request identifying at least one payee (0084, which discloses that the system requires that all authorized payees be specified in advance; 0134, which discloses that the user's authorization certificate would list the confirm to address of the payee);

a list of specific payees to whom the user identified in the user-identifying information is authorized to make payments **(0084, which discloses that the system requires that all a*uthorized payees be specified in advance; 0134, which discloses that the user's* authorization certificate would list the confirm to address of the payee);**

8. Brown discloses the method comprising:

generating information, with the one or more processors associated with the one or more computer systems operated by an organization, authorizing the payment request in response to a validation of the authority information included within the received certificate when the at least one payee identified in the payment request is included in the list of specific payee defined in the authority information included within the received certificate **(0169, which discloses that the certificate includes at least the *signer's name and public key…after the certificate is decrypte*d, the method continues by *determining whether the signer's identity … matches the signer's name in the decrypted* certificate, if not the signature verification service 710 terminates with the signature not being *verified…see claim 49, which discloses comp*leting the electronic payment request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80)**

9. Tallent discloses accessing a store of authority information that is coupled to the network, that is stored apart from the payment request and that is independent of the received certificate **(see figs. 1, 4C, 4D, 4E, 5, where authority is forwarded and verified by the root entity where authority to sign is stored; 0141-0148, 0167).**

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Fischer and incorporate a method comprising receiving, at one or more computer systems operated by an organization a payment request identifying at least one payee; a list of specific payees to whom the user identified in the user-identifying information is authorized to make payments; generating information, with the one or more processors associated with the one or more computer systems operated by an organization, authorizing the payment request in response to a validation of the authority information included within the received certificate when the at least one payee identified in the payment request is included in the list of specific payee defined in the authority information included within the received certificate in view of the teachings of Brown, Sudia and Tallent in order to ensure adequate security of the payment transaction.

10. As per **claim 10,** Fischer further discloses the method, wherein the payment request is for a predetermined amount and wherein authorizing the payment request further comprises authorizing the payment request when the maximum payment that the user identified in the user-identifying information is authorized to make is at least greater than or equal to the predetermined amount.

Brown discloses the method, wherein the payment request is for a predetermined amount and wherein authorizing the payment request further comprises authorizing the payment request when the maximum payment that the user identified in the user-

identifying information is authorized to make is at least greater than or equal to the predetermined amount (0177; 0183; 0184; 0185)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Fischer and incorporate a method wherein the payment request is for a predetermined amount and wherein authorizing the payment request further comprises authorizing the payment request when the maximum payment that the user identified in the user-identifying information is authorized to make is at least greater than or equal to the predetermined amount in view of the teachings of Brown, in order to ensure adequate authority of the user to issue the payment.

11. As per **claims 11, and 16**, Fischer further discloses the method, wherein the received

certificate conforms to the X.509 standard (col. 6, lines 60-67).

12. As per **claims 12, and 17,** Fischer failed to explicitly disclose the method, wherein the authority information included in the received certificate is configured as XML code.

Brown discloses the method, wherein the authority information included in the received certificate is configured as XML code (0062; 0068; 0069).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Fischer and incorporate a method

wherein the authority information included in the received certificate is configured as XML code in view of the teachings of Brown, in order to show the protocol used in the transaction

13. As per **claims 13, and 18,** Fischer failed to explicitly disclose the method, wherein the XML code is compliant with a DSML standard.

Brown discloses the method, wherein the XML code is compliant with a DSML standard (0062; 0068; 0069).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Fischer and incorporate a method wherein the XML code is compliant with a DSML standard in view of the teachings of Brown, in order to show the protocol used in the transaction

14. **Claims 29-33**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al U.S. Patent Application Publication No. 2004/0139327 A1 in view of Hwangbo U.S. Patent Application Publication No. 2003/0154376 A1 and Sudia et al (hereinafter "Sudia") U.S. Patent Application Publication No. 2002/0029337 A1 further in view of Tallent JR. et al (hereinafter "Tallent") U.S. Patent Application Publication No. 2006/0179008 A1.

15. As per **claim 29**, Brown et al discloses in a server computer to authenticate a user of a client computer and to verify that the user is authorized to request that the server computer carry out a requested action, the server computer comprising:

a processor **(see fig. 2, CPU 202; see fig. 5);** and

a memory coupled to the processor and configured to store a set of instructions that when executed by the processor causes the processor to:

receive a payment request along with a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field;

wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate defining access rights of the user including maximum payment that the user is authorized to make **(see figs. 1 and 3; 0165; 0067; 0174; 0183), including a maximum payment that the user is authorized to make and an indication of payees to whom the user is authorized to make payments (0183, which discloses *…the maximum signing authority of the signer…the digital certificate may specify a maximum signing authority… for example, a signer may only be authorized* to digitally sign**

requests up to $1000.00. Thus, the digital certificate of the signer will indicate a maximum signing authority of $1000.00); and

a list of specific payees to whom the user is authorized to make payments;;

retrieve from a store of authority information, stored authority information associated with the user of client computer, that is stored apart from the payment request and that is independent of the received digital certificate

validate the authority information within the received certificate based on a comparison between the retrieved authority information and the authority information included within the received certificate (**0088 which discloses that if a match is found, the signer is authorized for the corresponding role; 0169, which discloses that the certificate *includes at least the signer's name and public key…after the certificate is decrypted, the method continues by determining whether the signer's identity … matches the signer's name* in the decrypted certificate, if not the signature verification service 710 terminates with the *signature not being verified…see claim 49, which discloses completing the electronic payment* request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80**), and

generate information authorizing payment request in response to a validation of the authority information within the certificate when the at least one payee identified in the payment request is included in the list of specific payee defined in the authority information included within the received certificate (**0169, which discloses that the *certificate includes at least the signer's name and public key…after the certificate is decrypted,* the method continues by determining *whether the signer's identity … matches the signer's***

name in the decrypted certificate, if not the signature verification service 710 terminates with *the signature not being verified…see claim 49, which discloses completing the electronic* payment request when the payment amount does not exceed the signer's maximum authority; se also fig. 1, 2, 3, and 8; 0165; 0174; 0183; claim 80).

16. What Brown does not explicitly teach is:

a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and the extension field (Note: extension fields are inherent in X.509 certificates)

a list of specific payees to whom the user is authorized to make payments;

retrieve from a store of authority information, stored authority information associated with the user of client computer, that is stored apart from the payment request and that is independent of the received digital certificate

17. Hwangbo discloses a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and the extension field **(fig. 10; 0029; 0034; 0096; claim 17)**

18. Sudia discloses the method comprising:

a list of specific payees to whom the user is authorized to make payments **(0084, which discloses that the system requires that all authorized payees be specified in advance; *0134, which discloses that the user's authorization certificate would list the confirm to address* of the payee)**

19. Tallent discloses access a store of authority information that is coupled to the network, that is stored independent of the received digital certificate **(see figs. 1, 4C, 4D, 4E, 5, where authority is forwarded and verified by the root entity where authority to sign is stored; 0141-0148, 0167)**

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Brown et al and incorporate a digital certificate assigned to the user of the client computer, the digital certificate comprising a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion, wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and the extension field; a list of specific payees to whom the user is authorized to make payments; retrieve from a store of authority information, stored authority information associated with the user of client computer, that is stored apart from the payment request and that is independent of the received digital certificate in view of the teachings of Hwangbo, Sudia and Tallent respectively in order to ensure adequate security of the document and transaction.

20. As per **claim 30**, Brown further discloses the server computer, wherein the digital certificate conforms to the X.509 standard (0109; 0164; 0183)

21. As per **claim 31** Brown further discloses the server computer wherein the second code portion is configured as XML code (0062; 0068; 0069).

22. As per **claim 32**. Brown further discloses the server computer, wherein the XML code is compliant with a DSML standard (0062; 0068; 0069).

23. As per **claim 33**. Brown further discloses the server computer, wherein the authority of the user of the client computer is stored in a hierarchical authority data structure that is accessible by the server computer (0165 which discloses that the certificates are stored in an online, publicly accessible repository and are accessed using a standard protocol).

Conclusion

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Charles C. Agwumezie** whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Calvin Hewitt** can be reached on **(571) 272 – 6709**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3685
December 21, 2010